WGリーダー　齋藤正史

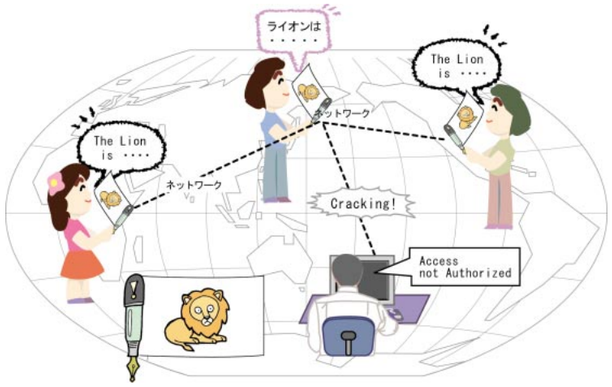


図１．万人が参加できる情報社会

1．20世紀の情報通信技術

汎用大型コンピュータでのバッチ処理からミニコンピュータを用いた時分割処理，そして複数のワークステーションを用いた分散処理を経て，個人用パソコンを用いた業務のサポートと協調処理へと私たちを取り巻く環境は変ぼう(貌)してきた。さらに，1990年代のWWWによるインターネットの急速な普及が，私たちの生活やビジネスのルールまで変革しようとしている。しかし，現状のインターネット情報サービスは，パソコンの操作や設定の複雑さなどが原因となり，パソコンが使える人々(＝情報強者)とパソコン操作の習熟度が低い人々(＝情報弱者)との間の格差を顕在化させている。また，英語で記述された情報が多く，母国語による情報格差も生じている。

こうした格差を埋めながらコミュニティ内での自由なコミュニケーションと情報アクセス環境を提供することが，次の20年の最重要課題であろう。パソコン以外の手段や道具による情報サービスへのアクセス，利用者の目的に沿って情報自体を変換しフィルタリングすることなどが重要な技術となる。小型軽量化された携帯電話は，電子メールやWebなどの情報サービスを取り込み，使用電力の限界と高機能化のトレードオフの中，確実にウェアラブルデバイスとしての地位を確立しつつあるが機能はまだ十分ではない。

2．21世紀初頭のコンセプト“万人が参加できるNetizen社会”

21世紀初頭には，言語，年齢，地理的制約，経済格差などの制約によらず，現状の情報弱者を含むすべての人がネットワークの住人“Netizen”として市民権を持てる情報社会が構築されていることだろう。**図１**に万人が参加できる情報社会のコンセプトを示す。また，構築のキーとなるコンセプトを以下に示す。

(1)　サービスアクセシビリティ

世界中のすべてのサービスにアクセス可能となる環境を整えるとともに，自分の属するコミュニティで自由にコミュニケーションを行う。

(2)　ウェアラブルデバイス

人が持ち歩く電子デバイスとコミュニケーションデバイスは一つに統合されていくだろう。例えば，紙のように薄くフレキシブルで携帯に便利なディジタルノートとも言うべきデバイスや巻取り可能な表示装置が組み込まれているペン型デバイス(ディジタルペン)が考えられる。表示装置の品質は現在の紙と同等以上で，直感的に使用できるユーザーインタフェースを備え，電池の寿命は１週間を超えることが望まれる。

(3)　情報の自動変換・抽出

国際的な情報交換を容易にするには，背景となる文化も考慮した言語の実時間翻訳が望まれる。また，アクセス可能な情報の量的増加に伴い，意味に基づく適切な情報の自動抽出が行われる。

(4)　ネット空間でのリアルな体験の実現

コンピュータとネットワークによる情報アクセスは地理的・空間的制約の解消に役立つが，これまでは，記号世界におけるコミュニケーションに限定されている。臨場感あふれる体験を提供する情報通信空間が望まれる。

3．実現のための技術課題と当社の取組

情報弱者が市民権を持てるNetizen社会の実現に向けての技術課題と当社の取組を以下に述べる。

(1)　サービスアクセシビリティ向上

アクセシビリティを向上するためのかぎ(鍵)は無線・有線通信技術とそれらの融合である。各種ネットワークは高速化・グローバル化・シームレス化し，真の意味での“網”を提供していく。当社は，長距離幹線系用波長多重(WDM)による40Gbpsクラスの高速伝送技術，第三世代携帯電話ネットワーク，低中高度軌道通信衛星ネットワーク技術の開発を進めている。

(2)　ウェアラブルデバイス

個人が持ち歩く情報デバイスは一つに統合され，その機能は電話，コンピュータ，個人認証，決済など多岐にわたる。デバイス形状は，ノート型やペン型だけでなく，ベルト，めがねのフレーム，財布，ヘアピン，手帳などが考えられ，ユーザーインタフェースについてもキー操作，音声，手書き入力など多様なものを提供していく必要がある。携帯電話端末の高機能化，軽量化，拡張性向上のための技術開発と情報理解(入出力と表示)にかかわる技術開発を進めている。

(3)　プライバシーとセキュリティ

現在の暗号技術は解読計算に時間がかかることを安全性の基にしているものが多いが，将来，計算量を低減させるアルゴリズムや量子コンピュータの開発が進んだ場合，暗号が短時間に解読されやすくなり安全性が問題となる。このような未来においても安心してコミュニケーションを行うことができる社会を築くためには，量子暗号化によるプライバシーとセキュリティの確保が必要である。当社は，線形解読法の開発，証明可能安全性を持つ秘密鍵暗号“MISTY”の開発，盗聴者検知が可能な量子暗号通信システム実現のための技術開発を進めている。

(4)　超分散サーバネットワーク

記号だけでなく意味までも含めた翻訳を行うためには，知識の理解・蓄積・抽出を助ける巨大で知能化されたデータベースが必要となる。**図２**に2020年の情報通信環境を示す。世界中に設置された超分散サーバが超高速通信インフラで接続され，ネットワークを構成し，双方向ディジタルネットワークやナノセルネットワークなどにシームレスに接続される。このネットワークが巨大で知能化されたデータベースとなり，感覚理解を用いた様々な形態の情報表現や高度の臨場感の実現，人間の思考を模擬した情報自身の進化，文化に関する知識のデータマイニングなどに利用されていく。

当社は，動画像からのオブジェクト抽出，自動インデックス付加を始め，メディアをまたがる情報の融合・変換，高速検索のための技術開発，コンピュータ間の高速接続技術開発を進めている。

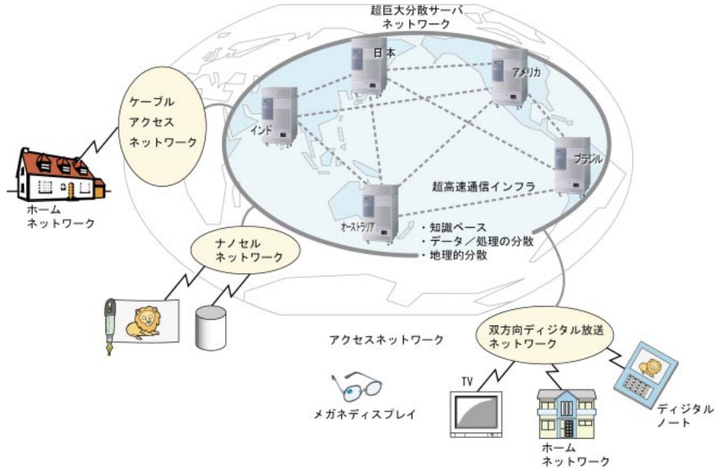
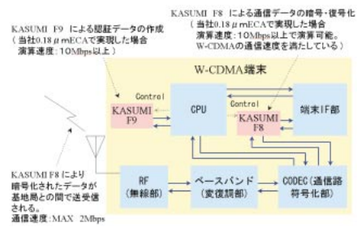


図２．2020年の情報通信環境

国産史上初の国際標準暗号“KASUMI（霞）”



W−CDMA端末におけるKASUMI使用例

当社は，1995年に新暗号アルゴリズム MISTYを発表し，以来，その安全性と小型・高速性は国内外から高い評価を受けてきた。99年には第三世代移動通信システム(W−CDMA)の国際規格を検討している標準化プロジェクト3GPP(Third Generation Partnership Project)においてその技術が国際標準暗号のベースとして認定され，移動通信システム用にカスタマイズされたものが新しくKASUMIとして誕生した。国産暗号技術が国際標準として単独で採用されるのは日本の暗号史上初めてのことである。また，各種W−CDMA端末の商用化のためIPのライセンス供与を2000年４月から開始した。このIPを用いると3GPPで規定されたf8，f9モードを用意し，各モード十数Mbps以上の高速で演算し，ゲート規模の超小型化も実現した(三菱0.18μmASICライブラリによる合成シミュレーション値)。